allies receive. For example, the United States has security-of-supply arrangements with nine other countries but not with Japan.[60] These agreements allow for the mutual supply of defense goods and services on a priority basis, when requested.

There are other examples too. Japan was also not included in an expanded National Technology and Industrial Base framework; the U.S. Congress pushed to include Australia, Canada, and the United Kingdom in this initiative to "bring together our closest allies and figure out a way to make progress in innovation and integration of our technologies."[61] Moreover, Japan has always remained outside some of Washington's closest intelligence circles—including the English-speaking intelligence-sharing framework (known as Five Eyes) established during World War II. Japan's absence from this framework has limited some sharing of counterintelligence information that is useful when evaluating the integrity of foreign researchers and investors. Most recently, in 2020, Japan was not included on a short list Washington drafted of countries that are excused from heightened levels of scrutiny with regard to FDI, although the door was left open for possible inclusion in the future.[62]

Defensive Technonationalism

It is worthwhile to assess some of the most important measures the U.S. and Japanese governments have employed to try to protect classified and proprietary information while keeping their technological edge.

Traditional Defensive Tools

Some technonationalist policies are defensive, designed to restrict other countries' firms and spies' access to technologies and industrial know-how deemed critical to a nation's security (economic or otherwise). In contrast, offensive tools are designed to proactively promote the competitiveness of domestic industries. At a certain level, defensive policies are always in place, usually to protect military technologies and secrets by employing a tiered classification system that limits access to specific individuals and companies that undergo an extensive clearance process overseen by central governments. Additionally, governments use special licensing requirements, export controls, and investment constraints to enforce a desired level of foreign access to intellectual property, products, or corporate control. Companies must comply with the minimum standards and approval processes that governments set, and they also can employ their own industrial security practices to protect trade secrets that in some cases go beyond government requirements.

The United States and Japan have used a variety of regulatory means to manage export controls for military and dual-use products during the technoglobalist era. For decades, the United States has governed defense-related exports with a munitions list that requires special licensing for certain products, services, and related data.[63] The items on this list are subject to a U.S. regulatory regime called the International Traffic in Arms Regulations (ITAR), which is overseen by the Department of State's Directorate of Defense Trade Controls. The oversight of this regime makes commercial transactions more complex and secure, but there is an important tradeoff: it can also limit sales of such products. When Congress placed U.S. satellites and related items on the munitions list in 1999, for example, the U.S. satellite industry lost about a quarter of its global market share over the next decade and arguably fell behind on the innovation curve.[64]

Items and services (including data) that are not considered munitions but that nonetheless have potentially sensitive commercial and military dual-use applications end up on a separate Commerce Control List regulated by the U.S. Department of Commerce. These export rules are not as cumbersome as ITAR, but such products still attract greater scrutiny depending on the import country and the specific import company or individuals involved. In this case, the proposed end use and end user are the primary concerns, rather than the product being sold. Finally, for certain end uses and users linked to possible cases of weapons proliferation, many countries—including the United States and Japan—use a catch-all system to make sure even unlisted items are not exported to certain people and places that might try to use the products for nuclear, chemical, or other weapons programs.[65]

Japan only began allowing defense equipment sales overseas starting in 2014 (effectively), and its exports are negligible compared to U.S. exports.[66] The few defense goods Japan exports must be approved by the Ministry of Economy, Trade and Industry's trade control department, and if the exports are politically sensitive enough, the National Security Council must decide. Like the United States, Japan uses a list approach for its high-tech exports (arms and dual-use items) and catch-all provisions. Both countries, along with forty others, implement their export rules in line with the Wassenaar Arrangement, an international agreement to apply certain standards of control and transparency related to arms and dual-use trade.[67]

Above and beyond export controls, protecting information from theft has become an increasingly important and difficult task for governments, private companies, and universities. In addition to its own classified information management system, the U.S. government created a National Industrial Security Program in 1993 to protect classified information as it contracts with the private sector and academia. The National Industrial Security Program Operating Manual (NISPOM) provides detailed requirements for how classified and unclassified information must be stored and transferred in

connection with a government contract. This manual also outlines a minimum level of investments in physical security, the management of subcontracts, and a wide range of other security-related details.

Japan generally handles such contract requirements on a ministry-by-ministry basis (rather than a national basis), a point that has generated some alliance friction when government-protected information is at stake and private companies are involved. U.S. government security clearances cannot be issued to foreign companies or even U.S. companies if they are under foreign ownership, control, or influence, unless the U.S. government is satisfied that the foreign connection poses no risk.[68] This stipulation can be mitigated by various means, including a special security agreement (SSA), although such bureaucratic safeguards add costs for the companies involved and will often limit a foreign management team's access to information related to the U.S. firm in question.[69]

The Nippon Telegraph and Telephone Corporation's (NTT) acquisition of Dell Services in 2016 required this kind of special security clearance permission, given Dell's existing contracts with the Department of Defense. Overall, Japanese companies have a good track record of concluding SSAs when necessary over the past two decades. But the Trump administration has indicated a desire to discriminate more aggressively against "foreign-owned producers" when it comes to national security, even if the producers are U.S.-based, so some Japanese executives are concerned that their investments could be somewhat curtailed.[70]

Export Controls Amid Broadening Conceptions of National Security

But government oversight of sensitive exports has expanded beyond the narrow purview of military applications and national security in recent years, a notable transition that underscores the resurgence of technonationalism. The U.S. government in particular has sought to extend the use of these export controls and classified information protections beyond pure military or weapons proliferation concerns to other specific technologies with the broader goal of protecting more general national economic or innovation advantages. A good example is the United States' Export Control Reform Act of 2018, which requires the Commerce Department to determine updated controls on certain "emerging" and "foundational" technologies that are "essential to the national security of the United States."[71] The department requested input from the U.S. public about how it should define these types of technologies, a policy development that will affect (among others) Japanese firms doing business in the United States and Japanese companies that utilize certain U.S.-made components and software.[72]

The Commerce Department's initial proposal in late 2018 worried a lot of business executives in the United States and globally.[73] The department received comments from over 230 companies and industry associations around the world.[74] These industry actors voiced apprehension that the proposal's new U.S. export licensing requirements would apply to too many items and would make cross-border research and production much more difficult and expensive.

Both U.S. and Japanese companies noted that these proposed changes could significantly restrict their joint research, product development, and trade involving a wide range of technologies. The department's initial proposal, for example, included several expansive "representative technology categories" such as biotechnology, AI, semiconductor technology, and additive manufacturing (including 3D printing).[75] Private sector respondents urged the Commerce Department to make a finer distinction between truly emerging technologies and many mature technologies that are already widely available. They also wanted the U.S. government to focus on the military applications of certain inventions (in terms of end use) instead of the underlying technologies themselves, so that many lucrative commercial uses would not be affected.

Other companies stressed the need to avoid restricting intracompany research collaboration that might take place across borders or involve joint venture partners based in other countries. Many Japanese and U.S. firms have mutually beneficial high-tech research centers in the other country. Such firms also often have facilities in India and other countries. Would these ventures all be treated the same way under this proposal? On a related note, several companies recommended that the Commerce Department avoid unilateral definitions of these technologies and seek broader multilateral consensus with other parties, including the European Union (EU), Japan, and others, so that market conditions would be optimized and private sector competition around the world would be fair and consistent.

This public criticism resonated with some Trump administration officials, leading to intense debates that lengthened the decisionmaking process.[76] It took the Commerce Department until January 2020—an entire year after its extended comment period closed—to decide on just one newly proposed rule, a provision restricting exports of AI-enabled geospatial imagery software.[77] Only Canada is exempted from new export licensing requirements for this technology, but, overall, this first decision on emerging technologies has reassured the U.S. and Japanese private sectors that the Commerce Department is unlikely to be hasty or sweeping in how it implements the mandates enacted in this reform. Instead of restricting AI-enabled software generally, for example, the rule was limited to the use of such software for digesting satellite imagery so that the stipulation would impact fewer firms and should allow for more timely license application reviews.

More disruptive and unpredictable has been the Trump administration's use of the so-called Entity List (another export control tool) to limit U.S. exports to China and undermine certain Chinese high-tech firms in the process. The Commerce Department uses the Entity List to require licenses for all U.S. firms' transactions involving a particular foreign company or individual, and the majority of listings tend to presume that such transaction requests would be denied. Originally focused on preventing the proliferation of weapons or the support of terrorist organizations in the late 1990s and early 2000s, Trump early on took aim at some of China's largest telecom and technology firms—first by placing the ZTE Corporation on the Entity List in 2016, then by targeting leading Chinese 5G conglomerate Huawei Technologies in 2019, and then by moving against AI champions including Hikvision and SenseTime in 2019.[78]

The Trump administration is pushing U.S. firms—and foreign firms that use a lot of U.S. technology—to distance themselves from these Chinese companies by threatening to cut off future transactions with these Chinese firms. (While Trump has continued issuing temporary general licenses that have exempt most transactions from the Entity List restrictions and have kept sales flowing through the early summer of 2020, these exemptions are being revisited every ninety days and could be rescinded whenever the administration chooses to stop issuing them.) The future impact of this policy is unclear but potentially significant if it forces supply chains to be realigned and ties between the world's two largest economies to be partially decoupled.[79] So far, the combination of exemptions and general licenses has moderated the effect. These exemptions allowed Huawei, for example, to actually boost its purchases from U.S suppliers by 70 percent in 2019, despite the nominal Entity List designation.[80]

Trump's Entity List decisions triggered a related debate about how much U.S. content a particular product is required to contain to qualify as a U.S. export subject to these special licensing rules. The Commerce Department currently applies its ruling to products with 25 percent or more of U.S. content by value, providing many U.S. companies with a way to evade the Entity List and keep selling to blacklisted Chinese firms even without a general license.

When China hawks in the Trump administration proposed lowering this de minimis rule to 10 percent for Huawei specifically (a level that frequently applies to a few sanctioned countries like Iran and North Korea), U.S. industry leaders pushed back and found a sympathetic advocate in the U.S. Department of Defense.[81] The Pentagon worried that lost sales could weaken U.S. firms' financial position and restrict their ability to invest in new technologies that the Defense Department relies on for next-generation weapon systems. China, after all, consumes about half of the world's semicon-

ductors and accounts for roughly one-third of U.S. semiconductor revenues. Losing this market could be damaging, although with supply chains in flux, it is possible that the firms that utilize these chips will disperse their manufacturing operations across more countries in the future.[82]

Yet other administration officials and some Republican senators were unmoved by the Pentagon's rationale. Senators Tom Cotton of Arkansas, Marco Rubio of Florida, and Ben Sasse of Nebraska wrote to Defense Secretary Mark Esper in January 2020 demanding an explanation: "Huawei is an arm of the Chinese Communist Party and should be treated as such," they wrote. "It is difficult to imagine that, at the height of the Cold War, the Department of Defense would condone American companies contracting with KGB subsidiaries because Moscow offered a discount." Other members of Congress raised similar concerns, and the Pentagon's opposition softened.[83]

The Trump administration eventually amended its foreign-produced direct product rule narrowly to require foreign companies that use U.S. semiconductor chip-making equipment—or otherwise make their products based on U.S. technology—to obtain U.S. licenses before selling their chips to Huawei and its affiliates.[84] U.S. firms worry that this decision will simply drive away their customers to other suppliers, and a lot will depend on how the rule is implemented. "There is a lot of lobbying going on right now in DC from the U.S. side," said one U.S. analyst.[85]

The Trump administration's defensive technonationalism vis-à-vis China has been most comprehensive in relation to Huawei, primarily because of its perceived lead in 5G telecommunications. As Democratic Senator Chris Coons of Delaware explained, "The very real potential that China will be the winner in this next generation of technology, and that will allow them to both exploit and benefit from and potentially disrupt what we be [sic] always on, always present, central networks that drive everything, from literally our vehicles, to health care, to national security, to our power system, is chilling and concerning."[86] Similarly, Democratic Senator Minority Leader Chuck Schumer of New York has said plainly that "allowing China to dominate global 5G networks threatens America's national security."[87] Brendan Carr, commissioner of the Federal Communications Commission, said that "we cannot treat Huawei as anything other than a threat to our collective security."[88]

Given this bipartisan sentiment in Washington, the U.S. government's pressure campaign against Huawei since 2016 has been aggressive—if episodic. In addition to the Entity List designation and the new amendment on restricting overseas chip exports to Huawei mentioned above, the U.S. government has prohibited federal purchases of Huawei's (and some other firms') equipment; has subsidized the removal of Huawei and other Chinese companies' equipment from U.S. rural telecommunications networks; and has filed legal charges against Huawei for alleged racketeering,

industrial espionage, and sanctions evasion.[89] A bipartisan group of U.S. lawmakers also submitted a bill in March 2020 that could deny Huawei access to the U.S. financial system, based on allegations that the firm covertly cooperates with the Chinese government in conducting espionage.[90] As Republican Senator Rick Scott of Florida described it, "we know Huawei is supported and controlled by the communist regime in Beijing, which continues to violate human rights and steal our data, technology, and intellectual property."[91]

The Trump administration has also been active—with support from Congress—in pressuring other countries to prohibit the use of Huawei equipment in their networks. Esper told NATO and other allies that "reliance on Chinese 5G vendors could . . . jeopardize our intelligence and communication-sharing capabilities, and by extension it could jeopardize our alliances."[92] Republican Senator Lindsey Graham of South Carolina added, "We are very firm in our commitment—Republicans and Democrats—that if you go down the Huawei road you are going to burn a lot of bridges." U.S. allies like the UK are wary of potentially burning such bridges, so London is exploring a more coordinated approach among like-minded countries—a so-called D-10 coalition that would involve the G7 nations plus Australia, India, and South Korea—to mitigate China's technology and supply chain dominance.[93]

Japan's Own Pace of Defensive Technonationalism

Japan also decided in late 2018 to limit the domestic use of Huawei products, but it did so more subtly than Washington did.[94] Tokyo prohibited potentially compromised equipment on government networks without mentioning specific company names. Japanese private firms seemed to understand the subtext, however, as mobile carrier and tech investor SoftBank subsequently took expensive steps to remove Huawei equipment from its own networks in Japan.[95] It is no wonder why Japan prefers a more subtle approach: although Tokyo wants to compete effectively with Beijing and limit technological and economic vulnerabilities as much as Washington does, China is still vital to Japan as a market and a manufacturing base, not to mention an imposing regional military power.

Indeed, in various ways, despite traditionally being considered a "paradigmatic case of techno-nationalism," Japan today is pursuing a more moderate approach than the United States.[96] Japan has hardly tightened its export control procedures amid Trump's Entity List designations, and when it has done so it is usually acting in concert with other nations, as it did with respect to military-grade cybersecurity software and manufacturing technology for weapon-capable semiconductor parts in 2020 under the Wassenaar Arrangement. Japan also quietly strengthened penalties for violating export controls in

2017.[97] When Japan has made headlines with unilateral moves on export controls in recent years, it has been either to relax rules for Japanese defense equipment exports (in 2014) or as part of a bilateral dispute with South Korea that had nothing to do with protecting domestic industry.[98]

When Japan has been more aggressive in other areas of defensive technonationalism—most notably by imposing additional restrictions on inward FDI and protecting national secrets and intellectual property—its actions have been due at least partially to encouragement or prompting from the United States. After Washington took steps to strengthen its FDI rules in 2018 (a step that the European Commission later took too), Japan amended its Foreign Exchange and Foreign Trade Act in 2019 to lower the purchasing approval thresholds (from 10 percent to 1 percent ownership of the company involved) for transactions in certain sectors that could pose national security risks.[99]

Readouts from the Ministry of Economy, Trade and Industry explaining the new investment rules highlight the "global trend to strengthen measures from the national security viewpoint," and, privately, Japanese officials worried that tighter U.S. standards could frustrate their companies' investments if they did not demonstrate stricter control themselves.[100] If a Chinese firm that posed national security concerns sought to acquire, say, a 5 percent stake in a Japanese firm, that transaction could disqualify the Japanese company from making investments of its own in the United States, unless the Japanese government could demonstrate that officials had carried out their own due diligence.

The coronavirus pandemic and the resulting economic stress have heightened concerns in Tokyo on this front, and a group of ruling lawmakers are considering new policies to make sure that smaller businesses with important technologies are not snapped up by foreign entities: "Economic security is just as important as military power," former economic revitalization minister Akira Amari said in a June 2020 interview.[101] More broadly, the Abe administration created a new economic security team within the National Security Council in April 2020 to manage policy coordination related to many of these types of technonationalist policies.[102]

These developments reflect the expansion of national security concerns to include safeguarding economic competitiveness and protecting domestic innovation. In the United States, this impetus produced the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018.[103] FIRRMA strengthened the role of CFIUS in reviewing any noncontrolling investment in U.S. businesses involved with critical technology—beyond defense interests—or collecting Americans' personal data. The biggest worry that triggered this policy shift has been the billions of dollars Chinese firms have sought to invest in innovative U.S. high-tech start-up companies.[104] FIRRMA also allows CFIUS to discriminate based on the source country of investment, which is how the Department of Treasury created exemptions for Australia, Canada, and the United Kingdom.[105] This special treatment was

credited to these three countries' "robust intelligence-sharing and defense industrial base integration mechanisms with the U.S." This is a level of U.S. confidence that the Japanese government aspires to reach.

A similar action-reaction interplay between U.S. and Japanese defensive technonationalism has been evident in terms of protecting classified information and intellectual property, as well as research integrity and security (including stepped-up scrutiny of scientists and researchers involved in projects on advanced technology). On this first point, U.S. officials have long complained to their Japanese counterparts that Japan's information security protections were inadequate, citing insufficient legal foundations for personnel clearances, the lack of a classified court system, and weak penalties for divulging secrets, among other critiques.[106] These issues have been discussed frequently in the U.S.-Japan Bilateral Information Security Consultations, which were created in 2007 following an incident in Japan that compromised some information about the U.S. Aegis radar system.

Many Japanese defense specialists and security-minded politicians subsequently have pushed for stricter and more uniform rules.[107] For some, the main goal is to improve Japan's national security capability for its own sake, but for many others it is about strengthening alliance cooperation. As Chief Cabinet Secretary Yoshihide Suga explained in 2013, "Japan can only share information with foreign governments on the presumption that Japan protects information by means of having proper laws in place."[108] Japan cannot afford to lose access to valuable U.S. intelligence.

The most significant step Japan has taken was enacting a new December 2013 law called the Act on the Protection of Specially Designated Secrets (or *Tokutei Himitsu Hō*). This legal change created an updated method for government offices to keep secret certain defense, diplomatic, or other information deemed vital to Japan's national security for up to thirty years initially, with the possibility of an additional thirty-year extension.[109] This law also covers secrets that other countries have shared with Japan. Its provisions stiffened penalties for divulging designated secrets and made the clearance process for government officials and some contractors more uniform.

But even this law has certain limitations. It did not centralize the clearance process, so each ministry has a degree of autonomy regarding how it follows the law. Failing a clearance review is extremely rare, as the government reported just one failed evaluation out of more than 150,000 people from 2015 through 2018.[110] A total of 412 state secrets have been designated by four ministries (predominantly by the Ministry of Defense and the Ministry of Foreign Affairs), and oversight mechanisms have detected fewer than ten procedural "violations."[111] It is possible that some of these violations are serious and involve divulging secrets, but Japan's lack of a classified court system makes prosecutors reluctant to pursue such accusations because they could not air classified evidence in public trials.[112]

A U.S. defense official described the Japanese reform as positive but "low hanging fruit" that leaves the information security system "too stove piped" and still requires program-specific SSAs in order to comply with U.S. standards for the treatment of confidential material related to new collaborative R&D initiatives.[113] Another official points out that—while the U.S. government has a unique and detailed professional classification for security specialists (GS-0080) across all departments including various specialties, grading positions, and training opportunities—Japan lacks such a professional cadre.[114]

Despite these limitations, overall, U.S. officials have applauded Japan's enactment of this new law as a step in the right direction and a good foundation for further reform. Combined with Japan's relaxation of its own arms export restrictions in 2014, the new law was seen as a way to enable closer U.S.-Japan defense industrial cooperation, but it quickly became apparent that Japan would probably need to take other steps to take full advantage of this reform's potential. One area that U.S. officials and company representatives emphasize consistently is strengthening Japanese industrial security, so that U.S. and Japanese firms could collaborate more seamlessly on government-sponsored projects that involve both classified and unclassified information.[115]

Partly to address U.S. concerns, Japan amended its Industrial Competitiveness Enhancement Act in 2018, creating a set of uniform standards for domestic industrial security and a process to certify that Japanese companies are meeting those general criteria.[116] U.S. officials also saw this as a positive step, but unlike NISPOM in the United States, Japan's new certification process only covers unclassified material and companies' proprietary information, not the protection of classified material in the private sector. Additionally, Japan's system is still ministry-by-ministry, so certification for a telecom company is slightly different than that for an aerospace company, because these sectors are regulated by different ministries. Moreover, the budgets of the firms overseeing the certification process come from fees submitted by applicant companies, creating some concerns about potential conflicts of interest. One U.S. industry executive observed that real change will come when Japanese firms view "higher levels of industrial security as an investment, rather than just a cost."[117]

When it comes to Japanese information security, it is possible to see the glass as both half-full and half-empty. Clearly, Japan has improved its information protection infrastructure and practices, and these improvements have enhanced information sharing between Washington and Tokyo. In addition to the examples already mentioned, the Five Eyes intelligence network is reportedly expanding cooperation with a few other trusted countries—including Japan—to address certain shared interests related to China and North Korea.[118] More regular interactions between Japan's Ministry of Economy, Trade and Industry and the U.S. Department of Defense are strengthening information sharing about supply chains related to China, among other improvements.

But a variety of remaining challenges—some already mentioned—make effective U.S.-Japan cooperation on technonationalist policies more difficult than it could be. Improving the Japanese clearance system and building a cadre of Japanese information security professionals would help significantly, because the hurdles to international collaboration are only getting higher. For example, the Department of Defense is elevating the cybersecurity requirements for companies that want to contract with the Pentagon, and these standards extend beyond primary contractors to include many of the subcontractors they enlist.[119] If small and mid-sized Japanese firms cannot keep up with the demands of the United States' new Cybersecurity Maturity Model Certification, they will have a harder time partnering with U.S. firms on defense-related business. Pentagon officials say that all Department of Defense contracts will contain these new requirements by 2026. Japan also lacks a classified patent system, making it and Mexico the only two G20 nations without one.[120]

U.S. officials also need to reevaluate certain aspects of their approach. Their current operating model could unnecessarily limit the pool of potential partners by creating ever stricter security requirements and providing little flexibility in terms of how those requirements are met. Industry executives from both countries complain that U.S. officials focus too often on prescriptive processes and equivalent bureaucratic structures or legal powers as a measure of foreign partners' compliance, without considering local laws, customs, or logistical parameters. Instead, they argue, the evaluation of firms' security measures should be based on whether the foreign partner's approach achieves an equivalent effect or outcome.[121] Such a reconceptualization would help both countries achieve a desired level of security while maximizing their available market opportunities.

A final area worth mentioning is heightened U.S. scrutiny of the integrity of scientific research from a national security perspective, particularly regarding Chinese researchers working in the United States or U.S.-based scientists collaborating with Chinese institutions (or what the Justice Department calls nontraditional collectors).[122] The Trump administration has placed new limits on Chinese graduate students' access to U.S. universities since 2018, shifting from five-year student visas to single-year visas for Chinese students in certain academic fields. In May 2020, Trump further suspended the entry of Chinese nationals for graduate education or research if they had any history of military affiliation.[123] The Trump administration has also cracked down on undisclosed affiliations with Chinese counterparts.[124] The Federal Bureau of Investigation arrested a Harvard professor in one high-profile case in 2020, and scientists from at least five other universities have been prosecuted since 2018.[125] In addition, a two-year probe by the National Institutes of Health led to fifty-four scientists losing their jobs or being fired for failing to reveal foreign funding ties—93 percent of which involved a Chinese institution.[126]

Supporters of this crackdown hail the progress and want even tougher measures to be enacted, but people responsible for R&D in the United States warn that the Trump administration could be driving talent back to China and India, leaving the United States shorthanded on skilled labor. In the fields of computer science, mathematics, and engineering, nearly 60 percent of the U.S. doctoral-level workforce is foreign born, and a report for the National Science Foundation urged "an evidence-based description of the scale and scope of problems posed by foreign influence in fundamental research," lest U.S. authorities overreact.[127] The ability of U.S. universities to carry out government-sponsored research or to partner with U.S. and Japanese industry actors could be negatively affected if things are taken too far.

U.S. officials raised these researcher assurance issues with Japanese counterparts at JHLC preparatory meetings in early 2019, looking to stimulate greater Japanese attention to these concerns and keep the allies in sync.[128] As with other issues including security clearances, industrial security, and cybersecurity, developing a truly harmonized allied approach on researcher assurance will be difficult due to various legal and cultural differences.

At just a logistical level, Japan's consulates and its embassy in China are not staffed properly to carry out the background reviews necessary to screen Chinese student visa applicants for these kinds of sensitivities, so they have to develop new ways to coordinate with Japan's National Policy Agency on these issues.[129] Moreover, as in the United States, some Japanese universities will be reluctant to completely accept the central government's perception of the threat that China poses and the costly restrictions that such policies require. In fact, at least a few universities have even embraced this as an opportunity to attract top Chinese talent, if the United States decides to reject them.[130] Needless to say, Japanese officials who share U.S. government concerns are dismayed by any downplaying of the risks associated with Chinese researchers and scientific funding, and they want to avoid a scenario in which a U.S.-blacklisted Chinese grad student winds up at a high-profile Japanese university.

Overall, U.S. and Japanese policymakers should be encouraged that they enter this new technonationalist era with similar threat perceptions and many common interests: they are already well-positioned to share sensitive information and align their defensive policies. Japan is close to being within the United States' most trusted circle of partners, but there is room to improve so that both countries can further maximize their position. The Trump administration is in danger of moving too aggressively and too unilaterally, and it would benefit from a more collaborative approach to designing and implementing these measures. Moreover, Trump will undermine his stated objectives vis-à-vis China if he does not stop applying punitive trade policies against allies and demanding exorbitant payments for alliance security cooperation. Japan, for its part, will need to take more significant steps to upgrade its technological and information security if it wants to take full advantage of its alliance with the United States, and this includes investments in its intelligence and defense enterprises.

A high-profile but soon forgotten bilateral initiative during the Trump-Abe era was the Japan-U.S. Economic Dialogue (from 2017 to 2019) led by Vice President Mike Pence and Vice Prime Minister and Finance Minister Asō Tarō.[131] This so-called Asō-Pence dialogue was an opportunity to tackle many of these challenging issues with a sense of urgency and a level of authority that is rare in bilateral relations, given the involvement of each nation's second-highest political leader. Instead, it became a forum for shadow boxing between the two sides over Trump's long-standing complaints about the U.S. trade deficit with Japan, even though the language of their joint statements suggested a much broader and more strategic approach.[132] Some constructive discussions did occur during its short tenure, but mutual suspicion about true motives and domestic infighting in both capitals produced very little from this exercise.[133] After the next U.S. presidential election, the winner would be well-served by trying again, but this time with a set of agreed-upon common objectives and priorities for these bilateral consultations.

Offensive Technonationalism

Successfully implementing well-targeted defensive technonationalist policies can help protect valuable intellectual property and contribute to allied competitiveness, but over the long term these defensive policies will yield few benefits unless they are combined with the effective promotion of U.S. and Japanese innovation and economic prowess. This capacity should be considered in broad terms, encompassing education, research and infrastructure investment, economic efficiency and resiliency, and collaboration with capable partners.

A more offensive mentality also includes leveraging cutting-edge commercial technology for national security purposes, something the Department of Defense tries to foster through its Defense Innovation Unit—started up in 2015—with offices in Silicon Valley, in Boston, in Austin, and at the Pentagon. In 2020, the unit's current head, Michael Brown, highlighted the importance of fielding a good offense: "We're focused too much on the defensive side, and that's the wrong balance," he said at a public forum, before recommending a big boost to government investment in scientific research and its enabling talent pool.[134]

The Trump and Abe administrations—like their predecessors—have produced a fair number of special commissions, analytical reports, and national strategies aimed at improving national competitiveness and innovation. Unlike before, these policy debates are trying to focus on multiple technological areas simultaneously even as the stakes and political tensions with China rise. The United States and Japan have produced multiple national strategies on AI, quantum science, cybersecurity, and space since 2017, together with various road maps and investment initiatives developed in cooperation with private sector business groups.[135]